Introducing:

Managed Security Services

Cybersecurity Metrics – Don’t Become a Statistic

73% of global brands suffered a significant DDOS attack in 2015 and 83% of those were attacked repeatedly.

Neustar's Third Global DDoS Attack and Protection Report

40% percent of cyberattacks are aimed at companies with 500 employees or less.

Jeff Bardin - Keynote speaker for NH Business Review and NH High Tech Council’s second Executive Series Forum on Cybersecurity (5/25/16)

Every day more than ***157 million*** attempts were made (via emails, browser searches, etc.) to entice our customers into connecting to risky URLs.

McAfee Quarterly Threat Report (Mar 2016)

3500% **Ransomware domains increased by a factor of 35 in the first quarter of 2016. The malware led to a collective loss of $209 million in the latest quarter of 2016 as opposed to $24 million for the entirety of 2015.**

Infoblox DNS Threat Index and FBI data

FBI officials are warning potential victims of a dramatic rise in the business e-mail compromise scam or “B.E.C.,” From October 2013 through February 2016, law enforcement received reports from **17,642 victims** and more than **$2.3 billion** in losses.

FBI Phoenix, April 4, 2016

$81 Million stolen from the Bangladesh central bank's account at the Federal Reserve Bank of New York. Swift CEO, Gottfried Leibbrandt, chief executive of the world's largest interbank funds-transfer system is surprised by extent of attacks.

The Wall Street Journal 6/3/16

Less than ***40%*** of organizations conduct full-network active vulnerability scans more than once per quarter.

2015 Cyberthreat Defense Report

67% rate as average or below the maturity of their in-house breach response skills in comparison to those of threat-actors targeting their organizations

FireEye 2015 Breach Preparedness & Response Study

Lessons Learned - Wanna Cry

Have Good back-up Policies

Ransomware is spread through Clicking on Malicious links and in payloads included in attachments

Frequent Vulnerability Scans

Patch often – keep you systems current

Keep your AV software up to date

Do not use unsupported Operating Systems such as Windows XP

Negotiating with Terrorists

October 17, 1995 - *U.S. Department of State Public Affairs Bureau*

- ***United States will not negotiate with Terrorists***
- ***United States will not pay ransom demands to Terrorists***

June 18, 2013 – G8 Summit Leaders signed agreement not to pay terrorists

- **Major industrial countries that view themselves as democracies**

Need to Change Culture of Blame

Sept 2017 – Equifax says CIO to Exit after breach

- ***Yahoo***
- ***IBM***
- ***Austrian Aerospace Company FACC***
- ***San Fransciso State University***
- ***Uber***
- ***Sony***
- ***Forrester***
- ***Target***

Key Take-Aways

1) **MSS is a DIR Shared Services Offer**

2) **18 Security Services Available: Only 2 have term limits**

3) **All Services Pre-negotiated by DIR**
    1) Includes the cost of HW/SW
    2) Established prices for each service
    3) SLA’s established and monitored by DIR

4) **Security Incident Management: No Retainer**

Managed Security Services Overview

Managed Security Services: Overview

Available Now!

What is Managed Security Services?

Managed Security Services (MSS) is an offering within DIR's Shared Services program, providing a cost-effective solution to state, local, municipal, and higher-education cybersecurity needs.

MSS is composed of three (3) Service Components, each containing multiple services to choose from to meet your IT security needs:

- **Security Monitoring and Device Management**
- **Incident Response**
- **Risk and Compliance**

Am I eligible for all MSS services?

Certain security services are included within the scope of the DCS infrastructure services contract and therefore cannot be procured separately for devices residing in a Consolidated Data Center (CDC) or covered by the DCS public cloud offering. An MSS FAQ and Service Matrix is available with specific details for you to determine whether certain services are available to your device(s), depending on their location.

http://dir.texas.gov/View-Contracts-And-Services/Pages/Content.aspx?id=45

Managed Security Services: Overview

Security Services

Security Monitoring and Device Management

- Security Information and Event Management (SIEM)
- Threat Research
- Security Operations Center Services
- Managed Endpoint Security

- Host Based IDS/IPS
- Network Based IDS/IPS
- Managed Firewall
- Managed Web App Firewall
- Malware Detection System

Incident Response

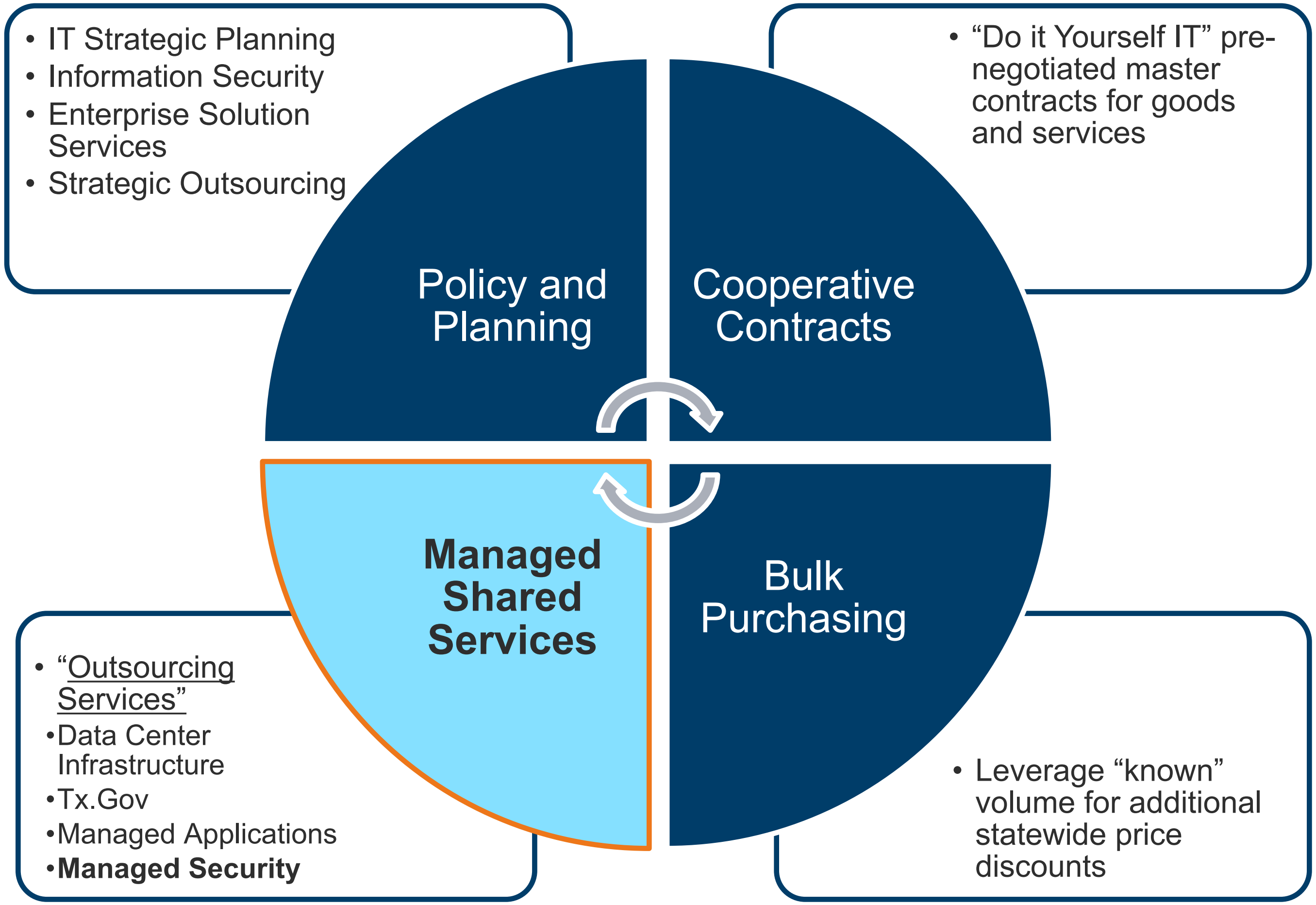
- Incident Response Preparedness
- Digital Forensics
- Security Incident Management

Risk and Compliance

- Penetration Test
- Web and Mobile Application Test
- Vulnerability Scanning
- Web App Vulnerability Scanning
- Risk Assessment
- Cloud Compliance Assessment

What is Shared Services?

DIR Shared Services: Managed Security Services Overview



- IT Strategic Planning
- Information Security
- Enterprise Solution Services
- Strategic Outsourcing

Policy and Planning

- “Do it Yourself IT” pre-negotiated master contracts for goods and services

Cooperative Contracts

Managed Shared Services

- “<u>Outsourcing Services</u>”
  - Data Center Infrastructure
  - Tx.Gov
  - Managed Applications
  - **Managed Security**

Bulk Purchasing

- Leverage “known” volume for additional statewide price discounts

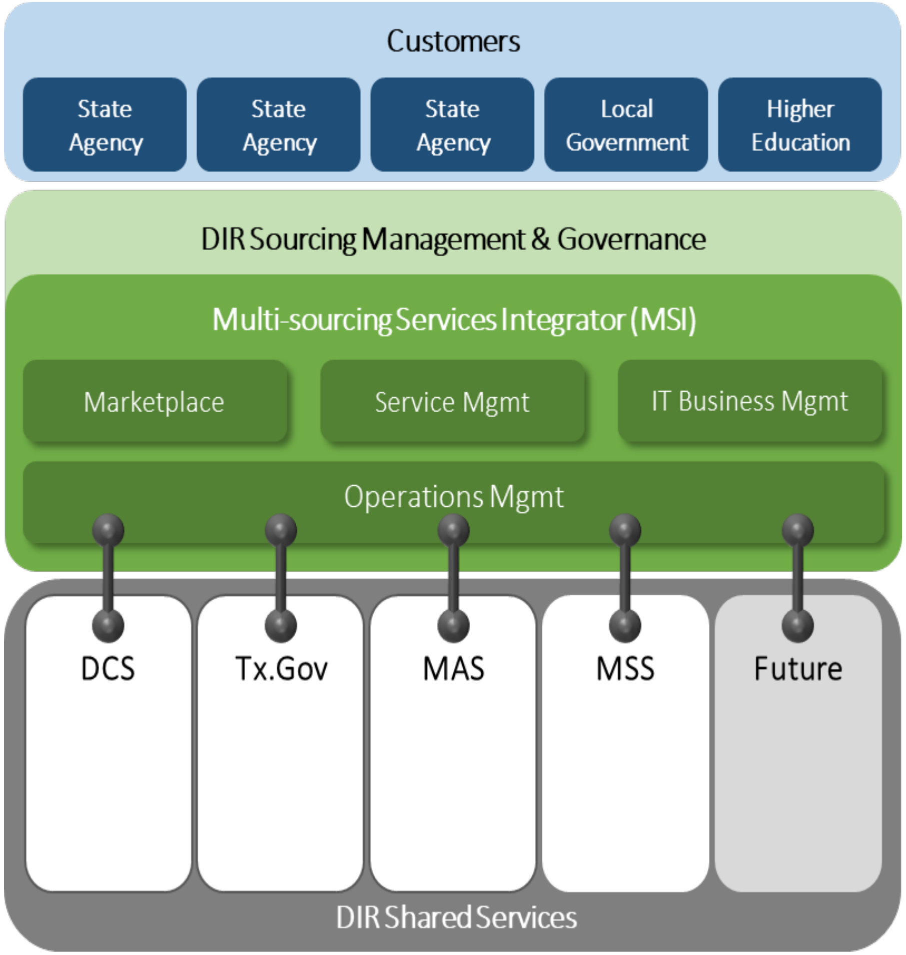
Eligible Customers

- State of Texas Agencies
- Local County and City
- K-12
- Higher Education
- Special Districts

What is Shared Services?

DIR Shared Services include an additional services integration layer for standard service delivery, integrating multiple service providers into a single platform to operationalize disparate services in a uniform and consistent way.

The Shared Services Portal provides for a single interface, whereby customers interact with all available service providers using standard processes for service onboarding, incident management, change management, SLA performance reporting, and consolidated billing.



How to Order

How do I Order Services?

New Customer - Initial Order

Step 1: Complete Customer Information Form (CIF)

Step 2: AT&T submits to DIR to initiate onboarding

Step 3: DIR begins 3 concurrent processes

- Process 1: IAC/ILC Execution
- Process 2: MSI Onboarding
- Process 3: Security Service Design

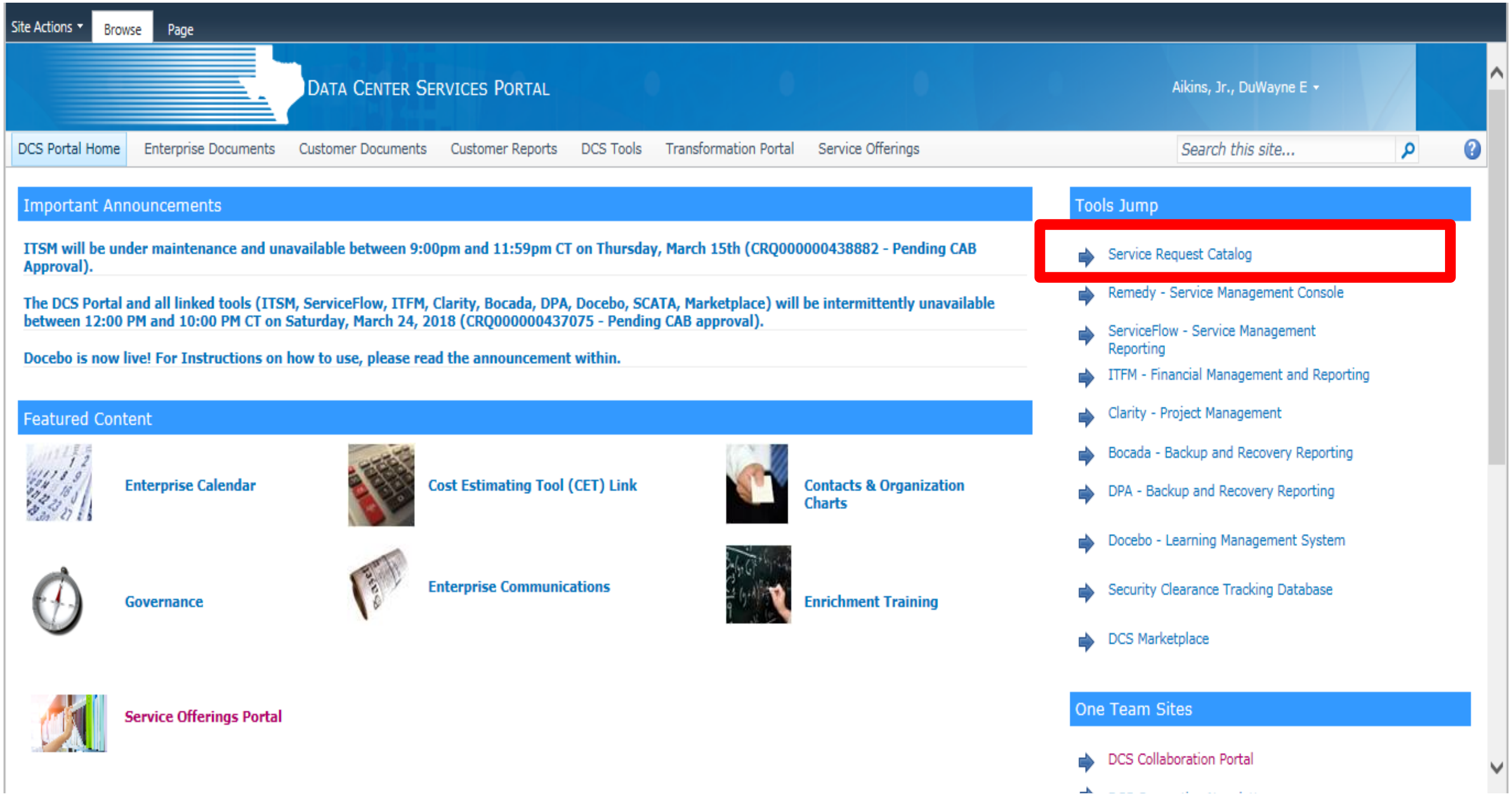
Existing Customer

Step 1: Log into Shared Services Portal

Step 2: Access Service Request Catalog

Step 3: Submit Request for Solution

Access Service Request Catalog



Important Announcements

ITSM will be under maintenance and unavailable between 9:00pm and 11:59pm CT on Thursday, March 15th (CRQ000000438882 - Pending CAB Approval).

The DCS Portal and all linked tools (ITSM, ServiceFlow, ITFM, Clarity, Bocada, DPA, Docebo, SCATA, Marketplace) will be intermittently unavailable between 12:00 PM and 10:00 PM CT on Saturday, March 24, 2018 (CRQ000000437075 - Pending CAB approval).

Docebo is now live! For Instructions on how to use, please read the announcement within.

Featured Content

- Enterprise Calendar
- Cost Estimating Tool (CET) Link
- Contacts & Organization Charts
- Governance
- Enterprise Communications
- Enrichment Training
- Service Offerings Portal

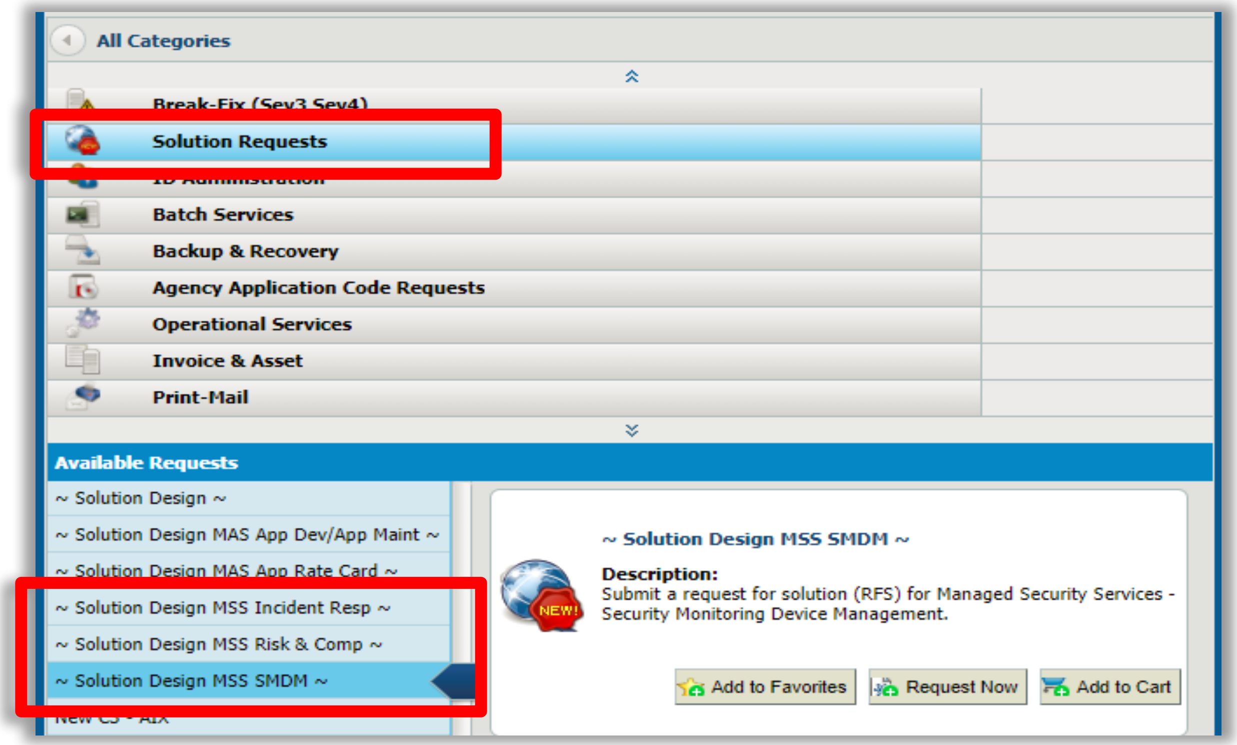
Tools Jump

- Service Request Catalog
- Remedy - Service Management Console
- ServiceFlow - Service Management Reporting
- ITFM - Financial Management and Reporting
- Clarity - Project Management
- Bocada - Backup and Recovery Reporting
- DPA - Backup and Recovery Reporting
- Docebo - Learning Management System
- Security Clearance Tracking Database
- DCS Marketplace

One Team Sites

- DCS Collaboration Portal

How to Order



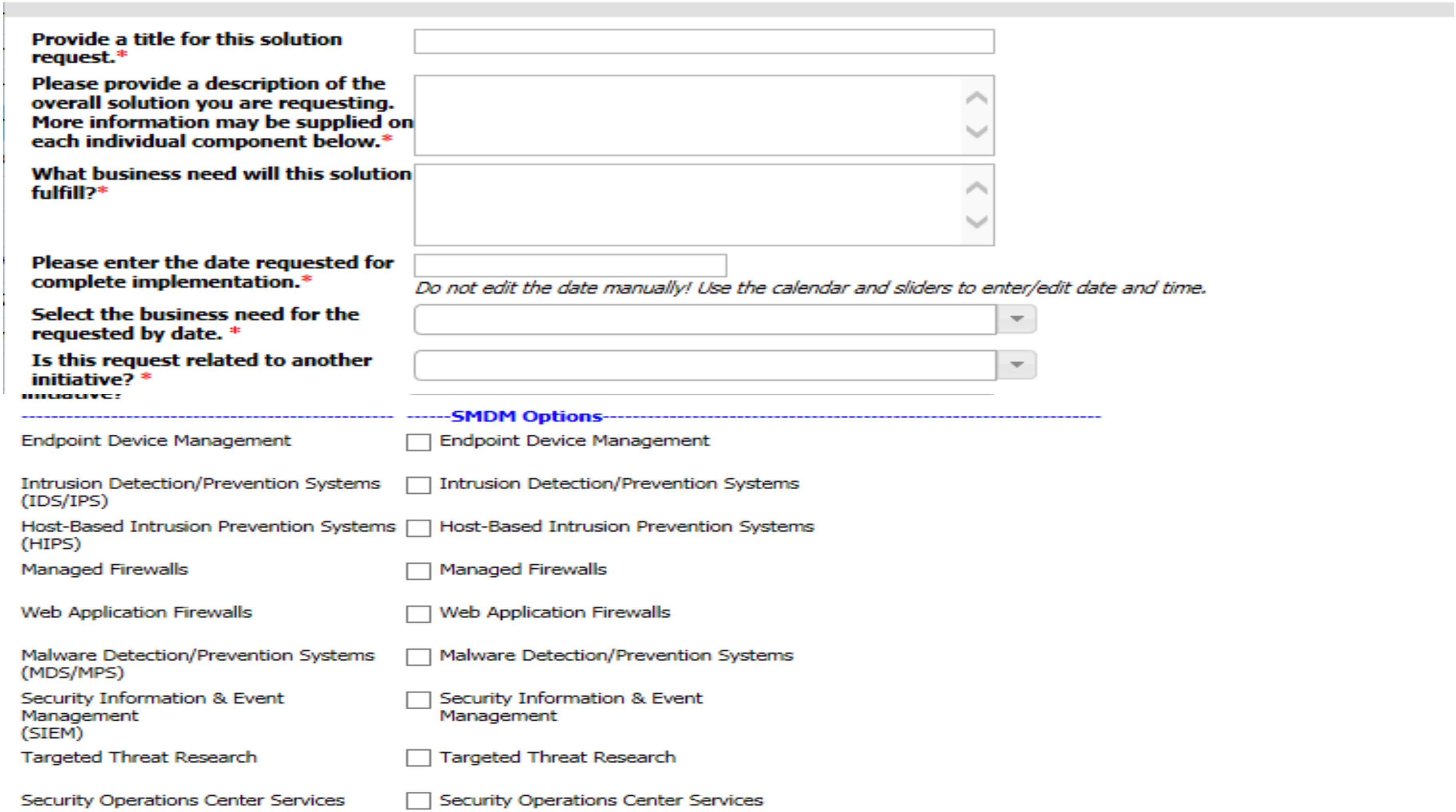
~ Solution Design MSS SMDM ~

Description:
Submit a request for solution (RFS) for Managed Security Services - Security Monitoring Device Management.

How to order Login to the DCS Portal

- Access the Service Catalog
- Select the **Solution Requests** category
- Select your desired MSS service to submit an **RFS request**:
  - Solution Design MSS Incident Resp
  - Solution Design MSS Risk & Comp
  - Solution Design MSS SMDM
- Complete the RFS form
- Click **Submit**

How to Order



Provide a title for this solution request.*

Please provide a description of the overall solution you are requesting. More information may be supplied on each individual component below.*

What business need will this solution fulfill?*

Please enter the date requested for complete implementation.*

Do not edit the date manually! Use the calendar and sliders to enter/edit date and time.

Select the business need for the requested by date. *

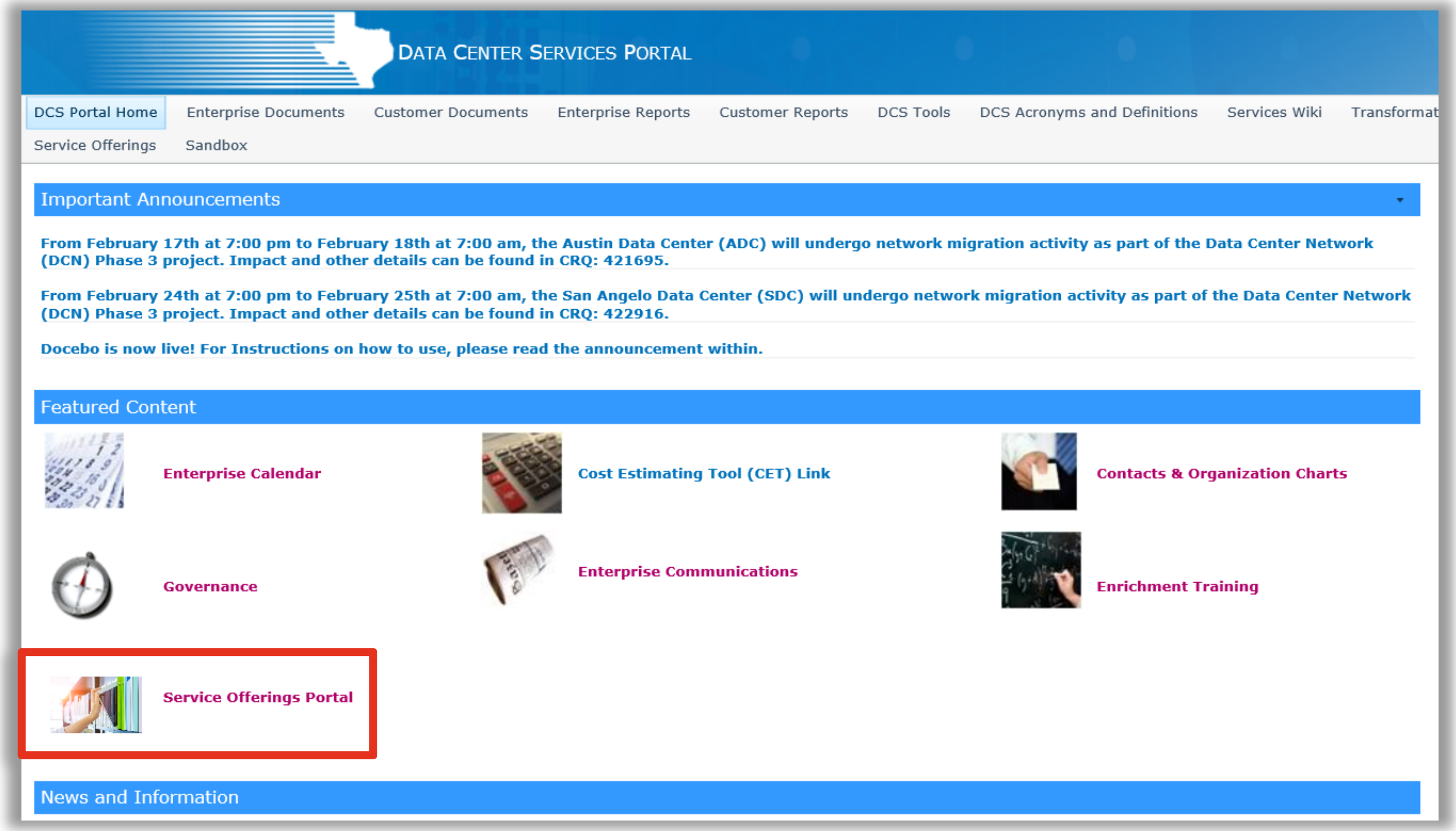
Is this request related to another initiative? *

------SMDM Options------

Endpoint Device Management	□ Endpoint Device Management
Intrusion Detection/Prevention Systems (IDS/IPS)	□ Intrusion Detection/Prevention Systems
Host-Based Intrusion Prevention Systems (HIPS)	□ Host-Based Intrusion Prevention Systems
Managed Firewalls	□ Managed Firewalls
Web Application Firewalls	□ Web Application Firewalls
Malware Detection/Prevention Systems (MDS/MPS)	□ Malware Detection/Prevention Systems
Security Information & Event Management (SIEM)	□ Security Information & Event Management
Targeted Threat Research	□ Targeted Threat Research
Security Operations Center Services	□ Security Operations Center Services

Where can I find more Information?

Where Can I Find More Information?



Important Announcements

From February 17th at 7:00 pm to February 18th at 7:00 am, the Austin Data Center (ADC) will undergo network migration activity as part of the Data Center Network (DCN) Phase 3 project. Impact and other details can be found in CRQ: 421695.

From February 24th at 7:00 pm to February 25th at 7:00 am, the San Angelo Data Center (SDC) will undergo network migration activity as part of the Data Center Network (DCN) Phase 3 project. Impact and other details can be found in CRQ: 422916.

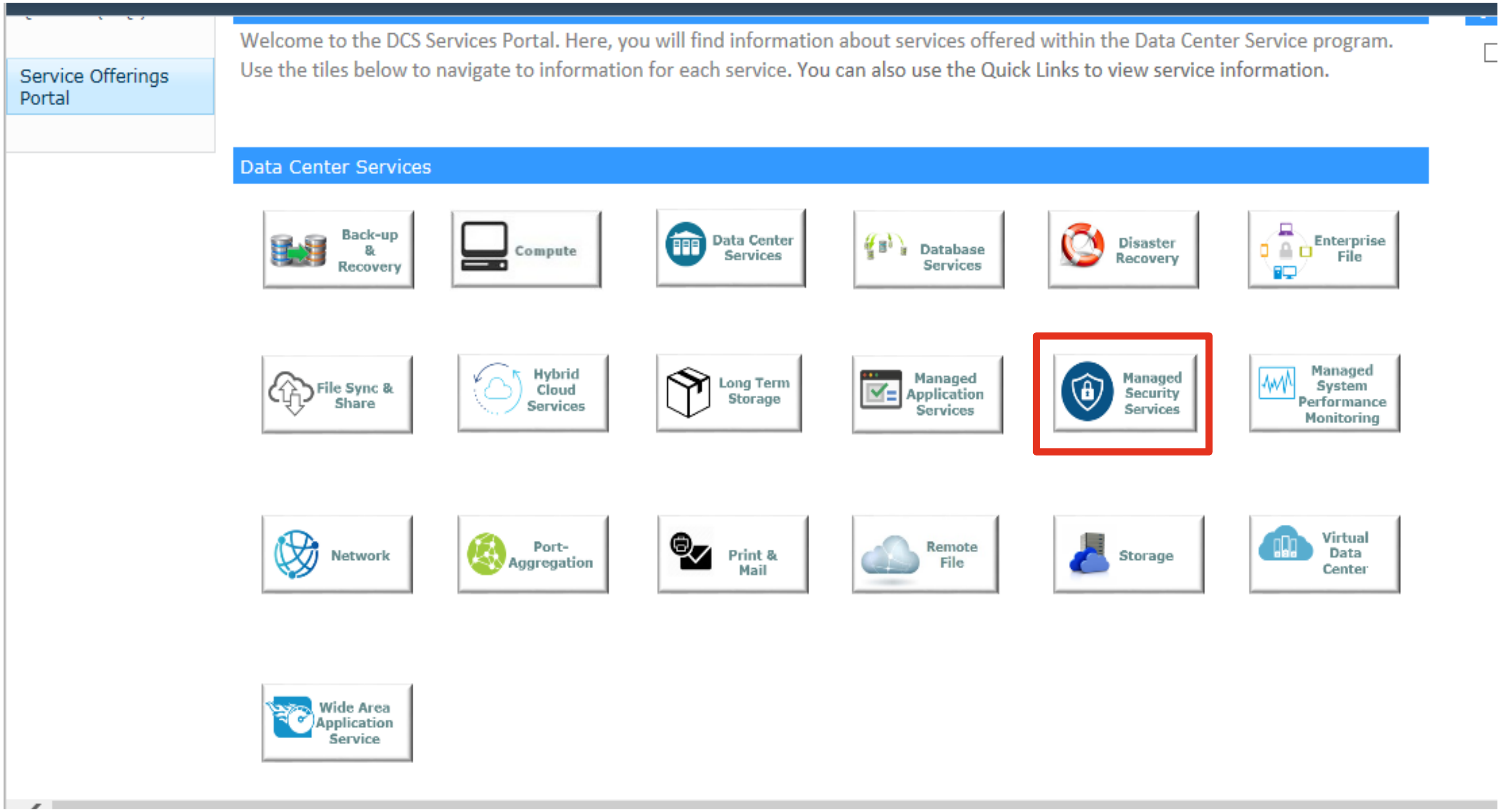
Docebo is now live! For Instructions on how to use, please read the announcement within.

Featured Content

Log into the DCS Service Offerings Portal.

Stay tuned to future DCS Update communications for announcements and locations to additional information.

Where Can I Find More Information?



Welcome to the DCS Services Portal. Here, you will find information about services offered within the Data Center Service program. Use the tiles below to navigate to information for each service. You can also use the Quick Links to view service information.

Data Center Services

What if I haven't been on-boarded yet?

1) Contact your local AT&T Client Executive
2) Send an email to texasmss@att.com

Incident Response Services

Incident Response Services

Incident Response Services

Incident Response Preparedness*

Provides a critical review of current internal processes and procedures for handling events, incidents, and evidence. Includes:

- Detective control configurations
- Deployed preventative and detective solution sets throughout the environment
- Current incident response plans
- Incident responder and handler skillset evaluations
- Incident responder and handler training evaluations
- Evidence seizure and storage procedure analysis
- Electronic data recovery
- Litigation support

Digital Forensics

- “On Demand” service
- Use of Encase and/or Carbon Black for analysis of hard drive images

Incident Response Management

- No retainer for this service
- Address adverse events, issues, or occurrences that may occur in your environment
- Includes detection, triage, response activities, and containment of computer security events

* **Important Note:** DCS Program customers already receive Incident Response services as part of your DCS assurances. However, if a security incident moves beyond the level of Atos contracted support to security incident analysis, the analysis can be performed by the MSS vendor (AT&T) upon Customer request.

Pricing Example: Incident Response

Example pricing is based on the Cost Estimation Tool (CET)

The Scenario:

Issue Profile

- Contained Breach

Service Need

- Incident Response Management

Resources Needed

- 2 Incident Engineers
- 1 Incident Engineer

Resource Hours Needed

- 40 hours onsite support
- 40 hours remote support

Pricing Overview:

Resource Unit	Unit of Measure (One-time)	Quantity	Cost per Hour	Total
Security Incident Management	Hourly Rate-Onsite	80	$208	**$16,640.00**
	Hourly Rate-Remote	40	$188	**$7,520.00**
Total Base Charges				**$24,160.00**
Total Complete Charges (after MIS and DIR Administrative fees)				**$25,712.00**

TEXAS
Data Center Services

Feedback / Q & A